



CVE-2017-9970

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-9970
State	PUBLIC
Assigner	cybersecurity@schneider-electric.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-12 23:29:00 UTC
Updated	2018-03-09 16:37:00 UTC
Description	A remote code execution vulnerability exists in Schneider Electric's StruxureOn Gateway versions 1.1.3 and prior. Uploading

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Schneider-electric	Struxureon Gateway	All	All	All	All

References

Reference	Source	Link	Tag
Schneider Electric StruxureOn Gateway CVE-2017-9970 Arbitrary File Upload Vulnerability	BID	www.securityfocus.com	Third Party
Schneider Electric StruxureOn Gateway CISA	MISC	ics-cert.us-cert.gov	Mitigation
Security Notification – StruxureOn Download Schneider Electric	CONFIRM	www.schneider-electric.com	Vendor
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[590560](#) Schneider Electric StruxureOn Gateway Remote Code Execution (RCE) Vulnerability (ICSA-18-046-04)

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report